Introduction to the National Information Exchange Model (NIEM)

NIEM Program Management Office

June 30, 2006
Document Version 1.0

NIEM
BRIDGING INFORMATION SYSTEMS

Table of Contents

Figures

Introduction

The vision for NIEM is to be the standard, by choice, for intergovernmental information exchange, thereby:

- Improving public safety and homeland security.
- Enhancing the quality of justice and decision making.
- Providing return on investment (ROI) to practitioners and vendors.

A variety of emergency situations in recent years have demonstrated in increasingly vivid detail the tragic consequences that often result from the inability of jurisdictions and agencies to effectively share information. Terrorist attacks, natural disasters, and tragic large-scale criminal incidents too often serve as case studies that reveal weaknesses in our nation's information sharing infrastructure. Even daily local events that involve multiple agencies, such as fire and law enforcement, illustrate the challenges to sharing information.

Citizens and decision makers alike largely believe that organizations today can instantly share critical information at key decision points throughout the whole of the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprise. Contributing to this problem is the portrayal of information sharing capabilities every day on television and in movies. Moreover, the level of integration that is possible today is evident in an ever expanding array of online services in commercial endeavors and consumer products (e.g., eBay and Amazon.com). Surely, first responders can share information and effectively communicate in emergency situations, when seconds count and lives are at stake.

NIEM is currently a partnership between the U.S. Department of Justice and the U.S. Department of Homeland Security.

The current domains in NIEM include justice, intelligence, immigration, emergency management, international trade, infrastructure protection, and information assurance.

It is an unfortunate reality that today enterprise-wide information sharing is not universally possible. Even though agencies perform similar operational functions, their internal business processes are inconsistent, and they continue to use different information systems and technology to support them. They lack a national mechanism to identify and facilitate information exchanges with other agencies and jurisdictions. As a consequence, these agencies are unable to effectively share information in a timely, secure manner, and too often, there are fundamental differences in the nature and understanding of information between them.

Courts, for example, have adopted sophisticated case management and jury systems. Similarly, law enforcement has adopted computer-aided dispatch solutions, mobile field reporting technology, and records management and crime analysis systems. The result is a series of information system silos that perhaps meet the internal operations and business practices of individual organizations but are not positioned to effectively share critical data with others in support of day-to-day operations and emergency situations.

An example of an emergency scenario demonstrates the breadth and scope of information sharing requirements in operational settings:

U.S. Border Patrol agents view a map of the area, displaying fixed locations such as landmarks and roads, agent locations, and the status of seismic sensors, on a vehicle-mounted or, when away from their vehicle, handheld device.

When sensor activation is displayed on the map, the nearest agent indicates that he will respond to it. The responding agent approaches the location and encounters a group of suspected undocumented migrants. He identifies himself as a U.S. Border Patrol agent and apprehends the majority of the group, but two men in the group escape. The agent radios a description of the two men and their direction, and the approximate last known position of the "got aways" is entered on the map so that other agents in the field can view it. A search is coordinated for the two migrants.

Meanwhile, information from a citizen's call about two suspected undocumented migrants loading into a pickup is entered on the map. The closest mobile unit pulls in behind the pickup. The agent immediately runs searches concerning the vehicle license plates, and after receiving positive results on the records checks, a traffic stop is affected.

The agent begins to question the driver and the two passengers and notices that the passengers match the description of the two "got aways" reported earlier. He runs the name and identification of each passenger in a federated query against local, state, and federal databases. The rapid response comes back with a positive history of immigration violations, as well as records of criminal violations. With probable cause established, the three men are taken into custody for further processing. When their fingerprints are run and other national databases are checked, one of the prisoners is found to be on a Terrorist Watch List, under a different name and identification.

Such an emergency situation requires a broad range of data exchange, communications interoperability, and closely aligned business practices. In this scenario, a significant range of information sharing is required to facilitate tightly coordinated response across multiple agencies, domains, and jurisdictions. The information provided in response to the queries originates in a number of databases, including local police, state Department of Motor Vehicle records, National Crime Information Center (NCIC), and the Integrated Automated Fingerprint Identification System (IAFIS), among others.

Today, while most of the same information is routinely retrieved, it must be done in a serial, labor-intensive manner, utilizing specific codes pertaining to each legacy system being queried. Too often agencies and jurisdictions lack the ability to securely share critical information in real time.

The National Information Exchange Model (NIEM) is designed to develop, disseminate, and support enterprise-wide information exchange standards and processes that can enable jurisdictions to effectively share critical information in both emergency and routine situations

As this scenario demonstrates, immediate, secure, enterprise-wide information sharing and interoperable communications are required. Similar information sharing is applicable regardless of whether the triggering event is an act of terrorism, a natural disaster, a major criminal incident, or simply the result of catastrophic structural failure. Similar scenarios can easily be constructed to demonstrate the range of information sharing that is inherent in the daily operations of border enforcement, passenger screening, port security, intelligence analysis, local law enforcement and judicial processing, correctional supervision and release, and other governmental functions. A scenario on emergency response to a national disaster can be found in Appendix A.[1]

[1] Additional sources for operational scenarios include the *National Planning Scenarios* and the NIEM pilot scenarios posted on www.NIEM.gov.

The Role of NIEM in Information Sharing

Rather than nationwide integration of all local, state, tribal, and federal databases, NIEM focuses on cross-domain information exchanges between communities of interest (COIs), across all levels of government—whether that is between individual local law enforcement agencies, law enforcement and emergency service agencies and other domains, or between local, state, tribal, regional, and federal agencies. As a consequence, not all data needs to be NIEM-compliant, only that data that is being shared across domains.

NIEM is a framework to:

- Bring stakeholders together to identify information sharing requirements in day-to-day operational and emergency situations.
- Develop standards, a common vocabulary, and an online repository of information exchange package documents (IEPDs) to support information sharing.
- Provide technical tools to support development, discovery, dissemination, and reuse of IEPDs.
- Provide training, technical assistance, and implementation support services for enterprise-wide information exchange.

NIEM was launched on February 28, 2005, through a partnership agreement between the U.S. Department of Justice (DOJ) and the U.S. Department of Homeland Security (DHS) Chief Information Officers (CIO). It leverages the data exchange standards efforts successfully implemented by DOJ's Global Justice Information Sharing Initiative (Global) and extends the Global Justice XML Data Model (Global JXDM) to facilitate timely, secure information sharing across the whole of the justice, public safety, emergency and disaster management, intelligence, and homeland security enterprise.

NIEM complies with the Homeland Security Presidential Directive (HSPD-5), which assigns the Secretary of DHS the role of principal federal official for domestic incident management. The Homeland Security Act of 2002 charges the Secretary with the responsibility for coordinating federal operations within the United States to prepare for, respond to, and recover from terrorist attacks, major disasters, and other emergencies. Building on this are a series of executive orders, which direct U.S. Government organizations to strengthen the sharing of terrorism information through the interchange of terrorism information between organizations and appropriate authorities of local and state governments and the protection of the ability of organizations to acquire this additional information.

NIEM complies with Section 1016 of the Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004. Based on this act, the President established the Information Sharing Environment (ISE) to facilitate the sharing of terrorism information. The ISE must to the extent possible, be supported by common standards that maximize the acquisition, access, retention, production, use, management, and sharing of terrorism information within the ISE, consistent with the protection of intelligence, law enforcement, military sources, methods, and activities. NIEM is identified by the ISE as a standards body, which provides a set of reusable common information standards.

To effectively exchange information across domains, there must be a common semantic understanding of data among participating agencies, and the data must be formatted in a semantically consistent manner. For example, two agencies may each gather information about persons charged with committing a crime. If the agencies share information regarding these persons, there must be a common understanding of the terminology each agency uses. One agency, for example, may refer to the person as the "offender," while another refers to them as the "defendant." Agencies do not necessarily need to entirely retool their information systems or adopt standards and coding schemes that impose an artificial uniformity in data collection that fails to meet their operational business needs, but there must be common understanding and semantic consistency in the structure of the data that crosses agency lines if it is to be successfully shared.

Information that is exchanged between agencies can be broken down into individual components—for example, information about people, places, material things, and events. Data components within an information exchange commonly shared and understood among all domains are identified as universal components (e.g., person, address, and organization), while components used in exchanges between multiple domains, but not universally shared, are identified as common components (e.g., offense, sentence, and disposition). Components managed by a specific COI (e.g., appellate case decision and arrest agency) are considered domain specific. Figure 1: NIEM Component Architecture shows the relationships between universal, common, and domain-specific data components, as well as the current scope of the NIEM domains.

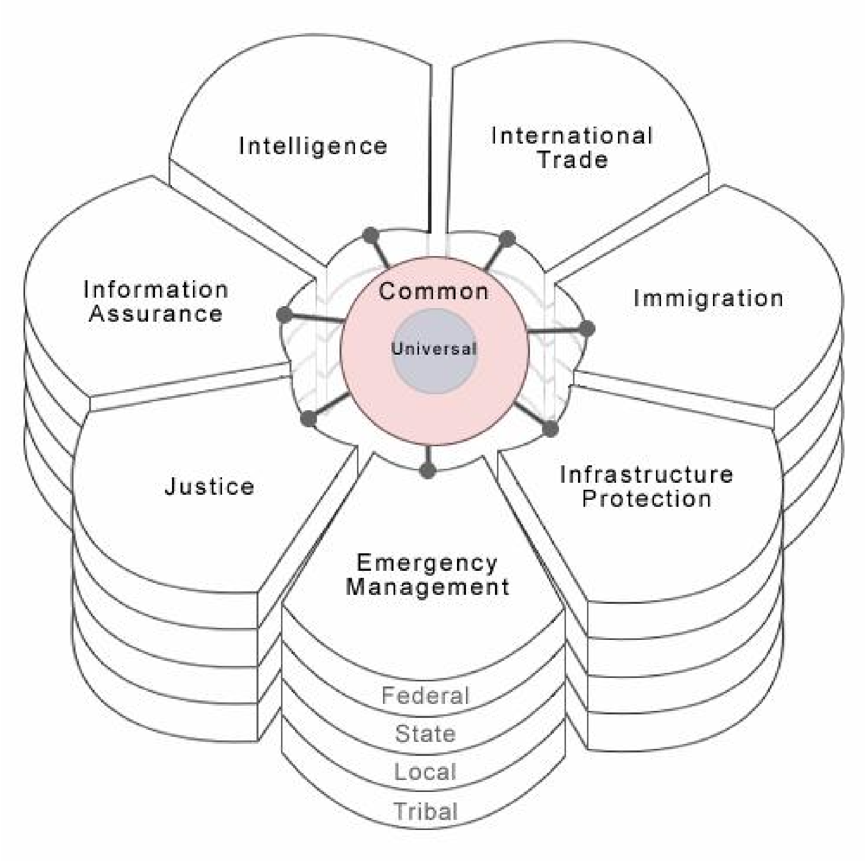
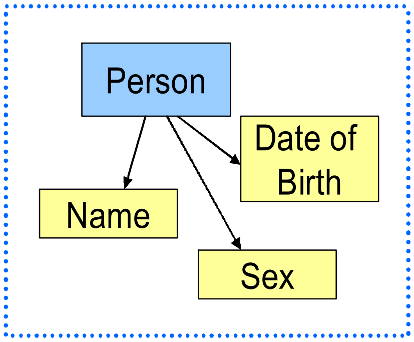


Figure 1: NIEM Component Architecture

A data component, such as a "person," represents a composite of attributes which describe something of interest—in this case, a *person*. The component may include such attributes as the person's name, date of birth, sex, race, ethnicity, height, weight, eye color, hair color, body type, etc. The *person* component is used in nearly all of the relevant agency or domain information systems that are today or may possibly be affiliated with NIEM, e.g., police information systems (where the person may be a suspect, an arrestee, a witness, or a victim), court case management systems (where the person may be a defendant, a plaintiff, a witness, an attorney, or a juror), health care systems (where the person may be a patient, doctor, or health care worker), transportation systems (where the person may be a passenger, a flight attendant, or other transportation worker).



Given this fact, *person* was chosen for classification as a *universal component* for purposes of NIEM. Once the *person* component has been defined and validated in operational use, it can be stored in NIEM and made readily available for discovery and reuse by other interested COIs. As a consequence, COIs need not spend the time and effort ordinarily required to construct a component from scratch, and it facilitates greater information sharing, making connections more expansive and expedient.

The full collection of information exchanged between agencies can be captured in an information exchange. For example, information regarding the arrest of a person will include not only descriptive and personal identification data regarding the individual—the *person* component described above—but also information about their alleged offense, the location of the offense, arresting officer, etc. An information exchange supports a specific set of business requirements in an operational setting. Additional information regarding this specific exchange can be further documented in the form of Information Exchange Package Documentation (IEPD), with data describing the structure, content, and other artifacts of the information exchange.

IEPDs include:

- Exchange specifications, such as schemas, wantlists, and style sheets.
- Documentation, such as business requirements, memorandums of understanding, domain models, use-case models, and business rules.
- IEPD specifications, including the manifest (list of artifacts in the IEPD) and the metadata registered with the IEPD.

COIs will continue to develop information exchange standards particular to their individual domains, and these standards will likely identify additional candidates for common and universal data components for NIEM.

Moreover, NIEM encourages and pursues participation of additional relevant COIs, such as health care and transportation. Through communication, outreach, and governance, stakeholders will be brought together to elaborate information exchange scenarios; map and model information exchange requirements; and will be provided with the operational methods, tools, and support services for development of their domain-specific components.

Understanding the Value of NIEM

Operational stakeholders and practitioners from all levels and branches of government are directly involved in NIEM, as are private sector solution providers, in designing these enterprise-wide information sharing capabilities.

NIEM's primary value propositions include:
Improving public safety and homeland security by enabling real-time and precise information exchange between COIs at all levels of government. Because NIEM models, builds, and documents reusable tools for enterprise-wide information sharing, operational agencies will be better informed and more capable of making decisions that can translate into direct improvement in public safety and homeland security.

- Enhancing the quality of justice and decision making by providing accurate, timely, complete, and relevant information to decision makers across the broad spectrum of NIEM COIs.
- Achieving greater efficiency, effectiveness, and return on investment (ROI) in operations and decision making by providing users with a set of reusable data components, as well as the tools needed for discovering and developing common and universal data components for effective information exchange. NIEM will provide significant ROI to practitioners by accelerating information exchange design and development through effective discovery and reuse of existing standards operationally validated in relevant COIs. Moreover, additional improvement in efficiency and effectiveness can be achieved through the application of standard methodologies for scenario-based planning, information exchange mapping and modeling, and standards development.
- Reducing the design and development time needed to build and implement robust, agile information sharing capabilities using NIEM's common standards, vocabulary, reusable data components, and tools. Additionally, NIEM will supply a data repository to host IEPDs and ensure interoperability between systems. NIEM will provide significant ROI to commercial solution providers by accelerating information exchange design and development through effective discovery and reuse of operationally validated standards.
- Facilitating business transformation by identifying and documenting information exchange requirements among diverse COIs, building information sharing standards, and enabling reengineering of key operations, where effective.

- Providing a valuable framework, infrastructure and governance that is scaleable beyond the current domains for other cross-government information exchange challenges.

A comprehensive Performance Management Plan will include the requirements and processes for regularly documenting and measuring the core business value of NIEM in building information sharing capabilities in each of the dimensions noted above. It will include specific, objective, quantifiable metrics associated with the NIEM value propositions, as well as metrics associated with the number of agencies using NIEM and the number of IEPDs registered and adopted by more than one agency. Reports will be used to document the outcomes (actual results) of these measures by the appropriate governance bodies that oversee program resources to ensure they provide value.

NIEM Processes

There are three sets of processes associated with NIEM from the perspective of a COI, Practitioner and of IEPD development. The COI processes include how a new COI joins NIEM, data insertions, external standard adoption, participation in NIEM governance activities and domain management. The Practitioner processes include the search, discover and extension of IEPDs, gap analysis, and the extension of IEPDs. These processes along with other support processes (e.g., NIEM Model Updates and Management, Issue Resolution, and Quality Assurance) are described in the NIEM CONOPS. This section describes the IEPD development processes, as shown in Figure 2: NIEM IEPD Development.

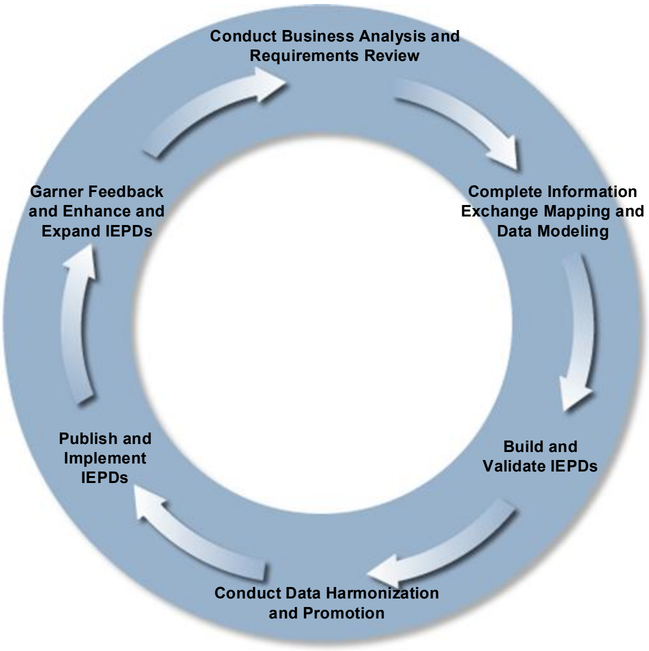

Conduct Business Analysis and Requirements Review
Complete Information Exchange Mapping and Data Modeling
Build and Validate IEPDs
Conduct Data Harmonization and Promotion
Publish and Implement IEPDs
Garner Feedback and Enhance and Expand IEPDs

Figure 2: NIEM IEPD Development

NIEM IEPD development has six steps:

- *Conduct Business Analysis and Requirements Review:* This step defines the business requirements associated with an information exchange for which NIEM is used. It incorporates scenario-based planning, which is the recommended methodology for elaborating the business context of events, incidents, or circumstances in which information exchange takes place.
- *Complete Information Exchange Mapping and Data Modeling:* This uses established methodologies to map and model operational information exchanges. Moreover, it describes the process a COI follows to map its

data sources to NIEM and identify IEPDs available for reuse and/or gaps between its data source and NIEM. COIs can use the NIEM repository to search and discover existing data components to decrease the time needed to construct IEPDs.

- *Build and Validate IEPDs:* This step addresses the importance of using common documentation standards, such as IEPDs, to ensure there is consistency in the way information is captured, stored, and exchanged and that uniform methodologies exist to support the generation of the IEPDs. Once the COI validates its IEPD, it may submit the IEPD to its domain specific area (proceed to Step 5) or nominate data components for inclusion into universal or common (proceed to Step 4).
- *Data Harmonization and Promotion:* The appropriate NIEM governance stakeholders form a team to review an IEPD submission and determine whether any of the data components should be included in universal or common. The team evaluates the submission and makes a recommendation regarding which, why, how, and when to integrate the proposed changes into NIEM.
- *Publish and Implement IEPDs:* Once an IEPD is approved, it is stored in the NIEM repository. Other stakeholders or COIs can then search and discover published IEPDs for reuse or extend for a specific instance of the information exchange.
- *Garner Feedback and Enhance and Expand IEPDs:* This step describes how the COIs work with the NIEM Program Management Office (PMO) to ensure existing IEPDs remain up to date and compliant with NIEM.

How NIEM Functions

NIEM includes a set of operational processes and procedures, standards, documentation, tools, training, and technical assistance which support each step in the NIEM IEPD life cycle (see Figure 3: NIEM Overview).

- *Documentation* includes the NIEM Concept of Operations (CONOPS), User Guide, and NIEM Naming and Design Rules (NDR).
- *Standards* include IEPDs and other process standards identified in supporting documentation.
- *Training and Technical Assistance* is facilitated by the NIEM Web site, training materials, in person instruction, executive materials, as well as a help desk.
- *Tools* include those used for activities such as scenario-based planning, information exchange mapping and modeling, and IEPD generation.
- *Governance and Processes* include the structure to manage and maintain NIEM and the processes and procedures behind its operations.

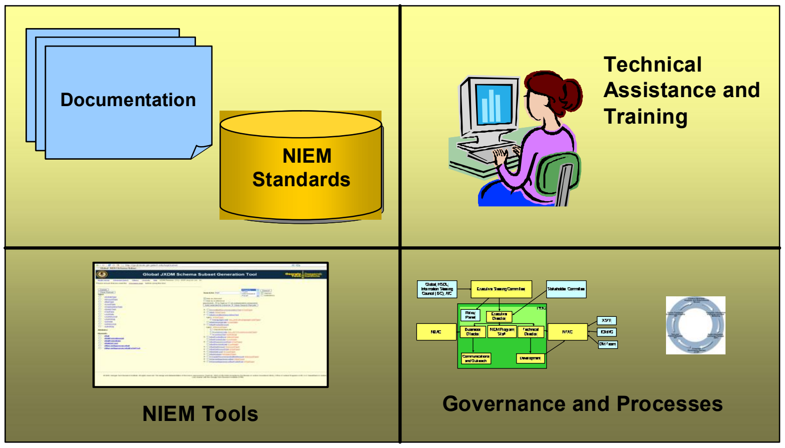


Figure 3: NIEM Overview

NIEM documentation and standards include a data dictionary, data model, and IEPDs. The data dictionary is a well-defined vocabulary of data names and structures. The data model is the body of concepts and rules that underlie the structure of the data dictionary, including data components arranged by domain, the type of data being represented (date, integer, Boolean, string, etc.), and a semantically precise, context-rich definition of each component. Together the data dictionary and model become a database, from which XML schemas are generated. These schemas contain the data components that are reused to construct the IEPDs.

NIEM standardizes the artifacts necessary for interagency information exchange into an IEPD. NIEM makes available reusable IEPD content used in data exchanges; creates and disseminates tools to support rapid IEPD development and deployment; and provides managed processes for the creation, support, dissemination, and implementation of information exchanges. In order to support these exchanges, NIEM provides a:

- Central place that allows for the registration and discovery of IEPDs
- Means to ensure IEPDs are developed using an established, conventional method that results in machine readable, easy-to-understand artifacts
- Place where IEPDs, certified by authoritative sources, can be highlighted and disseminated

NIEM's operations are dependent upon its stakeholders. NIEM is leveraging the work already started by its stakeholder, such as the Global JXDM. It functions to bring stakeholders of relevant communities together to define information exchanges and provide them the necessary tools and support mechanisms to facilitate adoption of common standards for enterprise-wide information exchange. NIEM stakeholders include those who are involved via the governance of the NIEM program. These include the executive steering committee (ESC), policy advisory panel, NIEM program management office (PMO), and stakeholder committee. More information on the NIEM governance structure can be found in the NIEM CONOPS.

Other stakeholders include executives, practitioners, program managers, subject-matter experts, technologists, product developers, academia, standards bodies, sponsors, media, and private industry—each of whom bring unique perspectives and contribute important content to the NIEM development efforts. These stakeholders comprise the COIs responsible for developing, harmonizing, and managing the data components found in NIEM.

Broad-based participation is critical to provide needed vision and effective decision-making direction for NIEM. Representatives from all relevant COIs, spanning all levels of government, can participate in NIEM.

As shown in Figure 4: COI Interaction With NIEM Governance Structure, COIs primarily interact with the NIEM Business Architecture Committee (NBAC), which has the responsibility to represent the business interests of related COI disciplines, identify business scenarios and information exchanges, and recommend data components such as universal and common. The NIEM PMO and ESC provide oversight through this process. Several COIs, such as the Global Justice Information Sharing Initiative (Global) and the Homeland Security Operations Center (HSOC) have been identified under the Federal Advisory Committee Act (FACA) as the authoritative bodies to provide guidance related to specific business areas and across jurisdictions. HSOC, for example, represents over 35 agencies, ranging from local and state law enforcement to federal intelligence agencies, and acts as the nation's nerve center for information sharing and domestic incident management—dramatically increasing the vertical coordination between local, state, tribal, territorial, federal, and the private sector partners. These COIs, established by FACA, provide specific advisory services to the ESC. Finally, representatives from the COIs technical team may work with the NIEM Technical Architecture Committee (NTAC), as needed, to resolve technical issues. The NTAC is primarily responsible for coordinating architecture with COI partners, working with external standards bodies, overseeing parallel information exchange efforts, and managing technical issues that arise.

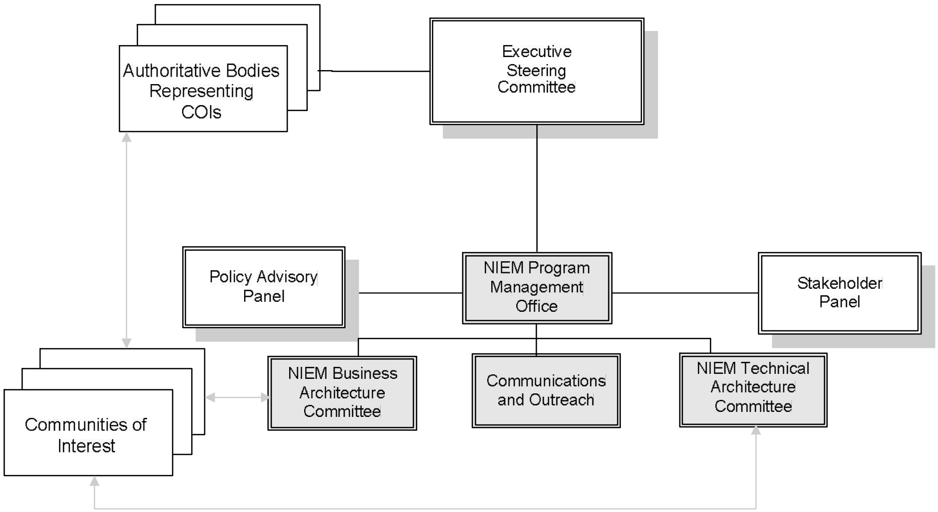

Authoritative Bodies Representing COIs
Executive Steering Committee
Policy Advisory Panel
NIEM Program Management Office
Stakeholder Panel
Communities of Interest
NIEM Business Architecture Committee
Communications and Outreach
NIEM Technical Architecture Committee

Figure 4: COI Interaction with NIEM Governance Structure

NIEM recognizes that the development of successful solutions to improve critical information exchange requires a focus on user needs and requirements. This means ensuring the appropriate input of both practitioners and policymakers across disciplines, jurisdictions, and levels of government, who are able to represent their own needs and to strategically approach the greater needs of their respective communities.

NIEM Near-Term Goals

NIEM development is an iterative process. The processes, standards, documentation, and tools that are part of NIEM will continue to be reviewed and updated as NIEM grows in scope and scale. Moving forward, NIEM efforts will concentrate on:

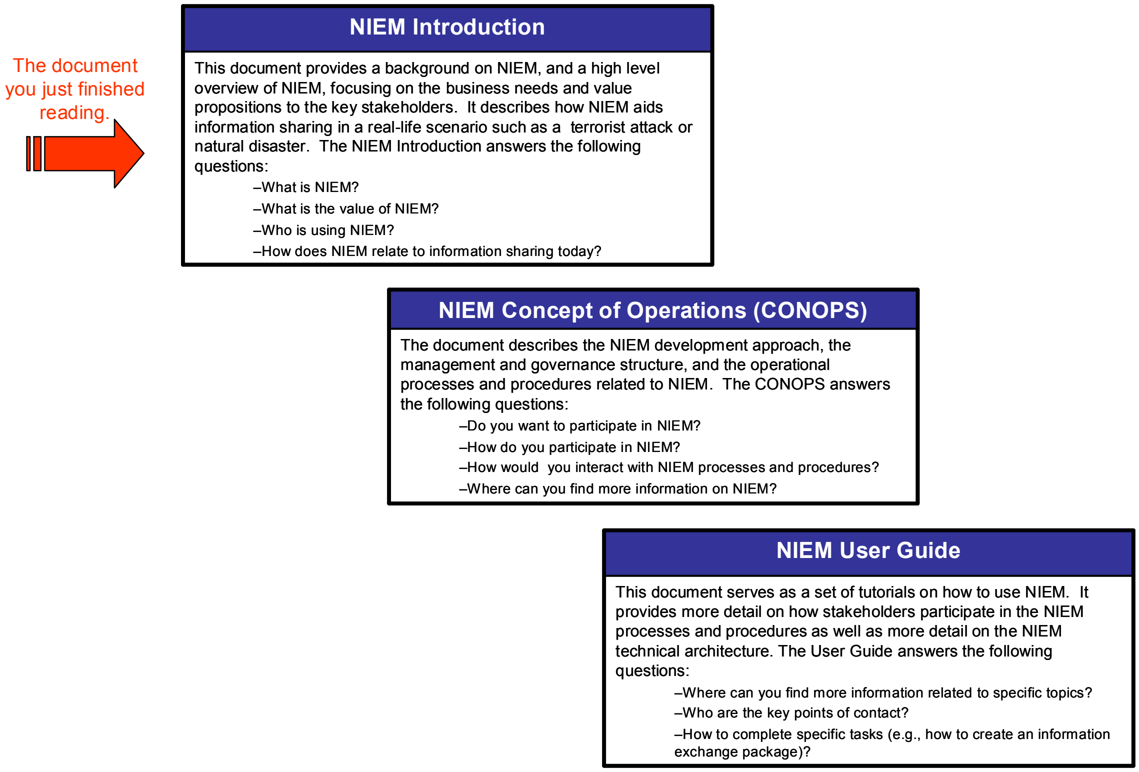
- *Core Capability Development and Maintenance:* This effort focuses on delivering NIEM 1.0 and subsequent releases; fully implementing NIEM governance; representing the critical mass of justice, homeland security, and intelligence information exchanges in their associated domains; developing a tools road map based on user requirements and delivering the tools into operation; and launching outreach activities (including the Web site), conference presentations, and training.

- *Information Exchange Standard Development:* This effort focuses on developing families of IEPDs, representing core, priority business areas at the national level. The initial focus areas will include incident reporting, people screening, suspicious activities, cargo screening, emergency and disaster management, and case management. Policies and processes will be developed to support creating, modifying, and implementing these standards. Nothing in this statement precludes COIs from championing and developing information exchange standards within their domains or for multiple COIs to do so cooperatively, with direct sponsorship from the NIEM PMO. They will follow the NIEM IEPD development process.

- *Outreach and Implementation:* This effort focuses on identifying additional pilots at the local, state, and tribal levels, targeting the emerging information exchange standards mentioned above, and implementing the infrastructure needed for training and technical assistance, including a help desk.

Conclusion

This introduction to NIEM is designed to provide a general description of the core capabilities of NIEM, the need for and value of NIEM as an information sharing enabler, brief descriptions on how NIEM operates and is governed, and the near-term goals of NIEM. The *Introduction to NIEM* is the first in a series of three documents providing stakeholders the information they need to participate in NIEM. The *NIEM CONOPS* and *User Guide* will follow and are recommended for further review. Figure 5: NIEM Reading Road Map describes the nature and scope of each of these documents.



The document you just finished reading.

NIEM Introduction

This document provides a background on NIEM, and a high level overview of NIEM, focusing on the business needs and value propositions to the key stakeholders. It describes how NIEM aids information sharing in a real-life scenario such as a terrorist attack or natural disaster. The NIEM Introduction answers the following questions:

–What is NIEM?
–What is the value of NIEM?
–Who is using NIEM?
–How does NIEM relate to information sharing today?

NIEM Concept of Operations (CONOPS)

The document describes the NIEM development approach, the management and governance structure, and the operational processes and procedures related to NIEM. The CONOPS answers the following questions:

–Do you want to participate in NIEM?
–How do you participate in NIEM?
–How would you interact with NIEM processes and procedures?
–Where can you find more information on NIEM?

NIEM User Guide

This document serves as a set of tutorials on how to use NIEM. It provides more detail on how stakeholders participate in the NIEM processes and procedures as well as more detail on the NIEM technical architecture. The User Guide answers the following questions:

–Where can you find more information related to specific topics?
–Who are the key points of contact?
–How to complete specific tasks (e.g., how to create an information exchange package)?

Figure 5: NIEM Reading Road Map

Appendix A: Emergency Response Scenario

The 911 Emergency Operations Center (EOC) of a mid-sized urban jurisdiction begins receiving telephone calls from residents regarding what is variously described as a fire, an explosion, and a partial building collapse of a 25-story building in city center. The calls quickly escalate in number and urgency and are received from residents of the affected office building, local residents of other nearby buildings, and cellular telephone calls from pedestrians and passing motorists.

The EOC dispatches police, fire units, and emergency medical personnel. The cause of the damage and the fire, as well as the extent of the damage and scope of the emergency, takes time to establish. First responders arriving on scene begin reporting back to the EOC on the nature and scope of the damage, which is extensive and may well result in a catastrophic collapse of the entire building and potentially extensive damage to surrounding buildings. Initial on-scene units find the aftermath of a significant explosion with several ongoing fires and many “walking wounded” wandering throughout the incident scene.

Establishing lines of communication and sharing information with relevant local, state, and federal agencies are crucial. First responders must coordinate their actions to secure the scene and ensure the safety of residents and responding units to: rescue, treat, and transport victims for medical treatment; extinguish fires and stabilize the site; share information with local government and state and federal officials; marshal resources; share relevant data with local hospitals, civil defense, environmental authorities, the media, and federal agencies; recover bodies and evidence; and begin investigations to apprehend and detain suspects (if necessary).

Police and fire initiate a command post across the street from the incident location. Police units establish a critical perimeter for public safety entry only and begin initiation of a secondary perimeter using Geographic Information Systems (GIS) mapping. Emergency Medical Services (EMS) set up an initial triage contiguous to the police and fire command post. Initial injured are assessed, and information is forwarded to area hospitals via devices that are tracking hospital capacities, services available, and patient transports.

Real-time video feeds are transmitted from the scene to the command post. Personnel location technology is in use providing 2D/3D location and biotelemetry of fire and police personnel to their command staffs, as well as monitoring of immediate air quality in proximity to the explosion site. Upon completion of the first search, the scene is declared unsafe and messages are sent to all on-scene personnel to remain outside of the critical perimeter until the scene is cleared by the bomb squad. The media is kept informed of progress, as appropriate.

The EOC uses a combination of networks to disseminate critical information to police, fire, and emergency personnel, as well as health and human service agencies, transportation authorities, border enforcement agencies, and civil defense units, including a) indications and warnings, b) incident notifications, and c) public communications. Notifications are made to appropriate local, state, and federal jurisdictional levels and to private sector and nongovernmental organizations through mechanisms defined in emergency operations and incident action plans at all levels of government. Geospatial information is used to integrate assessments, situation reports, and incident notifications into a coherent common operating picture.[2]

[2] Note: Portions of this scenario have been adapted from *NIMS Basic Communication and Information Management*, FEMA 501-5, March 29, 2006, Revision D, and *MESA TS 70.001 v. 3.1.2 (2005-01), Project MESA; Service Specification Group—Services and Applications; Statement of Requirement*, Annex C and Annex D, at http://www.projectmesa.org/ftp/Specifications/MESA_70.001_V3.1.2_SoR.doc.

Appendix B: Glossary

The following list is a subset of key terms and their definitions, which are necessary to understand the core concepts discussed in this document. The complete NIEM Glossary can be found on www.NIEM.gov.

- *Common Component:* A component that meets technical standards, complies with NIEM requirements, is common across one or more (but not all) participating domains, and is reusable.
- *Community of Interest (COI):* Authoritative sources responsible for developing, harmonizing, and managing the data components (vocabularies) found in interdomain exchanges.
- *Component:* An object, meant to interact with other objects, encapsulating certain functionality. For NIEM, component is normally used to reference data components contained in the NIEM data model and reused to construct IEPDs.
- *Data:* Facts represented in a readable language, such as numbers, characters, images, or other methods of recording, on a durable medium. Data on its own carries no meaning. Empirical data are facts originating in or based on observations or experiences. A database is a store of data concerning a particular domain. Data in a database may be less structured or have weaker semantics (built-in meaning) than knowledge in a knowledge base. Compare *Data* with *Information*.
- *Data Dictionary*: A set of metadata that contains definitions and representations of data elements.
- *Data Model*: A graphical and/or lexical representation of data, specifying their properties, structure, and interrelationships.
- *Data Repository:* Provides a discovery mechanism for a data dictionary and/or IEPD information. It includes descriptions of data structures (i.e., entities and elements) and may also include metadata of interest to the enterprise, data screens, reports, programs, and systems. Typically it includes an internal set of software tools, a database management system, metadata, and loading and retrieval software for accessing repository data.
- *Discovery:* The act of locating a machine-processable description of a Web service-related resource that may have been previously unknown and that meets certain functional criteria. It involves matching a set of functional and other criteria with a set of resource descriptions. For NIEM, discovery

normally refers to the search of IEPDs within a repository to identify data components that can be reused in IEPD development.

- *Domain:* A group that has the business requirement, desire, and capability to harmonize semantics (including structure) for the exchange of data.
- *Domain-Specific Components:* A component that meets technical standards, complies with NIEM requirements, and is specific to only one domain, which is managed and harmonized by a COI.
- *Extensible Markup Language (XML):* XML is a structured language for describing information being sent electronically by one entity to another. XML Schema defines the rules and constraints for the characteristics of the data, such as structure, relationships, allowable values, and data types. NIEM does not use document type definition (DTD); it only uses XML schemas.
- *Framework:* A specific implementation of a component architecture.
- *Governance:* The system and manner of providing authority and control.
- *Information:* Contextual meaning associated with, or derived from, data.
- *Information Exchange Package (IEP):* A set of data elements used to support the sharing of data within a particular business context. An actual set of data that is requested or produced from one unit of work to another.
- *Information Exchange Package Documentation (IEPD):* A collection of artifacts that define and describe the structure and content of an IEP.
- *Message:* The basic unit of communication between a requester and a provider and should encompass IEPDs relevant to the message exchange.
- *Naming and Design Rules (NDR)*: The NDR specifies an information sharing framework. These rules and principles are intended to establish and, more importantly, enforce a degree of standardization at the national level.
- *Repository:* An information system used to store and access architectural information, relationships among the information elements, and work products. For NIEM, the repository includes the data dictionary, data model, IEPDs, and the data components that comprise them.
- *Stakeholder:* A person or organization that has a legitimate interest in a project or entity; anyone with an interest (or "stake") in what the entity does.

- *Universal Component:* A component that meets technical standards, complies with NIEM requirements, is defined in universally acceptable terms across all participating domains, and is reusable.